UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/758,242	01/12/2001	Prabir Bhattacharya	9432-000128	7867

7590 07/09/2007

Harness, Dickey & Pierce, P.L.C.
P. O. Box 828
Bloomfield Hills, MI 48303

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	**PAPER NUMBER**
2131	
MAIL DATE	**DELIVERY MODE**
07/09/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/758,242	BHATTACHARYA ET AL.	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 April 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the communication filed on April 21, 2005. Claims 1-20 were originally received for consideration. Claims 21-24 have been added by the received amendment.

2. Claims 1-24 are now pending consideration.

Response to Arguments

3. Applicant's arguments with respect to claims 1-24 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

4. Claim 3 is objected to because of the following informalities: In the second limitation, the word "until" is misspelled "unit." Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-5, and 8-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leppek (U.S. Patent 5,933,501) in view of Watts (U.S. Patent 6,587,842).

Regarding claim 1, Leppek discloses:

A method for encrypting a data file content, the method comprising the steps:

encrypting the data file with a master key (column 4, lines 33-39), wherein a first encryption operating (master key) is used to encrypt the data;

generating one or more dual-encrypted blocks based on a set of secondary keys, the dual-encrypted blocks contained within the encrypted data file (column 5, lines 34-50), wherein the data is subsequently encrypted using multiple different encryption operators (secondary keys).

Leppek does not explicitly describe providing the encrypted data file and an attachment file to an authorized user, the attachment file enabling a device to access the data file content once for each secondary key. Watts teaches a system where an electronic message (e-mail) is transmitted to a customer along with an attachment "key-file" which has the keys necessary to access the encrypted data (Figure 2, column 4 lines 37 – 47). In the method of Leppek, the multiple encrypted data is sent over a network to a receiver which must possess multiple keys (decryption operations) to decrypt the multiple encrypted data. Leppek does not explicitly disclose the method of distributing the unique keys to the receiver, but Leppek reveals that two different keys would be

required to decrypt a twice encrypted data (column 6, lines 40-49). It was well-known at the time of invention that e-mails with attachment files are a common way to send data files to users. Leppek also discloses that the receiver needs the decryption operators in a correct order in order for the decryption to work properly (Leppek: column 6, lines 41-49). Therefore it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to each type of data with its corresponding key in an attachment file so that the data file could be decrypted if it is encrypted with more than one key that the receiver does not possess (Watts: column 52-55).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Leppek discloses:

The method of claim 1 further including the steps of:

randomly generating the master key (column 5, lines 7-13), wherein the encryption operator (key) are generated using an arbitrary sequence.

Leppek does not explicitly disclose hiding the master key within a data structure of the attachment file. Watts teaches hiding the key in the attachment file (Figure 6, column 5 lines 12 – 26). According to Watts, this hiding of the key makes it "extremely difficult to locate key information" (Figure 6). The hiding of the key makes the transmission of the keys more secure and makes the compromising of the key and the encrypted data difficult. Therefore it would have been obvious to one of ordinary skill in the art at the

time the applicant's invention was made to hide the key data within the attachment file to make the location of the key information extremely difficult.

Claim 3 is rejected as applied above in rejecting claim 2. Furthermore, Leppek discloses:

The method of claim 2 further including the steps of:

creating an odd logarithmic bit integer (column 5, lines 6-13); and

incrementing the integer by two until a prime number is found (column 5, lines 6-13);

said prime number defining the master key (column 5, lines 6-13), wherein the generation of the keys is open-ended and the algorithm used to generate them is a design choice.

Claim 4 is rejected as applied above in rejecting claim 2. Leppek does not explicitly disclose hiding the master key within a data structure of the attachment file using an NP-hard problem. Watts teaches hiding the key in the attachment file (Figure 6, column 5 lines 12 – 26). According to Watts, this hiding of the key makes it "extremely difficult to locate key information" (Figure 6). The hiding of the key can use any algorithm, and it is obvious to use the NP-hard problem algorithm as it was a well-known algorithm at the time of invention. The hiding of the key makes the transmission of the keys more secure and makes the compromising of the key and the encrypted data difficult. Therefore it would have been obvious to one of ordinary skill in the art at the time the

applicant's invention was made to hide the key data within the attachment file to make the location of the key information extremely difficult.

Claim 5 is rejected as applied above in rejecting claim 1. Furthermore, Leppek discloses:

selecting one or more continuous blocks to be dual-encrypted (column 5, lines 19-25);

randomly generating the secondary keys (column 5, lines 7-13), wherein the encryption operator (key) are generated using an arbitrary sequence;

generating a duplicate selected block for each secondary key in the set (column 5, lines 33-44);

generating dual-encrypted blocks based on the duplicate selected blocks and the secondary keys (column 5, lines 33-44);

inserting the dual-encrypted blocks into the data file (column 5, lines 33-44).

Claim 8 is rejected as applied above in rejecting claim 1. Leppek does not explicitly disclose receiving an email message from the attachment file and determining whether another message having the same status content has already been received. Watts teaches a system where an electronic message (e-mail) is transmitted to a customer along with an attachment "key-file" which has the keys necessary to access the encrypted data (Figure 2, column 4 lines 37 – 47). In the method of Leppek, the multiple encrypted data is sent over a network to a receiver which must possess

multiple keys (operators) to decrypt the multiple encrypted data. Leppek does not explicitly disclose the method of distributing the unique keys to the receiver, but Leppek reveals that two different keys would be required to decrypt a twice encrypted data (column 6, lines 40-49). It was well-known at the time of invention that e-mails with attachment files are a common way to send data files to users. Leppek also discloses that the receiver needs the decryption operators in a correct order in order for the decryption to work properly (Leppek: column 6, lines 41-49). Therefore it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to each type of data with its corresponding key in an attachment file so that the data file could be decrypted if it is encrypted with more than one key that the receiver does not possess (Watts: column 52-55).

Claim 9 is rejected as applied above in rejecting claim 8. Leppek does not explicitly state an attachment which has a status content that defines a current operational state and an identifier for the attachment file. Watts teaches a system where an electronic message (e-mail) is transmitted to a customer along with an attachment "key-file" which has the keys necessary to access the encrypted data (Figure 2, column 4 lines 37 – 47). In the method of Leppek, the multiple encrypted data is sent over a network to a receiver which must possess multiple keys to decrypt the multiple encrypted data. Leppek does not explicitly disclose the method of distributing the unique keys to the receiver, but Leppek reveals that two different keys would be required to decrypt a twice-encrypted data (column 6, lines 40-49). It was well-known at the time of invention

that e-mails with attachment files are a common way to send data files to users. Leppek also discloses that the receiver needs the decryption operators in a correct order in order for the decryption to work properly (Leppek: column 6, lines 41-49). Therefore it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to each type of data with its corresponding key in an attachment file so that the data file could be decrypted if it is encrypted with more than one key that the receiver does not possess (Watts: column 52-55).

Claim 10 is rejected as applied above in rejecting claim 8. Furthermore, Leppek discloses:

The method of claim 8 further including the step of storing the status content to a data storage medium (column 1, lines 65-67), wherein the encryption operators are stored in a database.

Regarding claim 11, Leppek discloses:

A method for enabling a device to access an encrypted data file content, the method comprising the steps of:

decrypting single-encrypted blocks of the data file with a master key (column 6, lines 15-20), wherein the master key is the first decryption operator (key) and if there is only one encryption operator applied, the first decryption operator (master key) is only applied;

decrypting dual-encrypted blocks of the data file with the master key and at least one secondary key in a set of secondary keys, where the set of secondary keys contains at least two secondary keys (column 6, lines 16-29), where a subsequent set of decryption operators is applied to the data that has been encrypted with multiple encryption operators;

repeating the decryption steps for each secondary key in the set of secondary keys such that the device is able to access the data file once for each secondary key in the set (column 6, lines 40-49), wherein the decryption process is iteratively repeated.

Claim 12 is rejected as applied above in rejecting claim 11. Furthermore, Leppek discloses:

The method of claim 11 further including the step of decrypting the blocks on a block-by-block basis such that the device only has access to the data file content one block at a time (column 6, lines 40-49), wherein the decryption process is iteratively repeated.

Claim 13 is rejected as applied above in rejecting claim 12. Furthermore, Leppek discloses:

The method of claim 12 further including the step of re-encrypting the single-encrypted blocks with a new master key (column 5, lines 34-42), wherein the encrypted data is re-encrypted with a new encryption operator (master key).

Claim 14 is rejected as applied above in rejecting claim 13. Furthermore, Leppek discloses:

The method of claim 13 further including the steps of:

randomly generating the new master key (column 5, lines 7-13), wherein the encryption operator (key) are generated using an arbitrary sequence.

Leppek does not explicitly disclose hiding the master key within a data structure of the attachment file. Watts teaches hiding the key in the attachment file (Figure 6, column 5 lines 12 – 26). According to Watts, this hiding of the key makes it "extremely difficult to locate key information" (Figure 6). The hiding of the key makes the transmission of the keys more secure and makes the compromising of the key and the encrypted data difficult. Therefore it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to hide the key data within the attachment file to make the location of the key information extremely difficult.

Claim 15 is rejected as applied above in rejecting claim 14. Furthermore, Leppek discloses:

The method of claim 14 further including the steps of:

creating an odd logarithmic bit integer (column 5, lines 6-13); and

incrementing the integer by two until a prime number is found (column 5, lines 6-13);

said prime number defining the master key (column 5, lines 6-13), wherein the generation of the keys is open-ended and the algorithm used to generate them is a design choice.

Claim 16 is rejected as applied above in rejecting claim 14. Leppek does not explicitly disclose hiding the master key within a data structure of the attachment file using an NP-hard problem. Watts teaches hiding the key in the attachment file (Figure 6, column 5 lines 12 – 26). According to Watts, this hiding of the key makes it "extremely difficult to locate key information" (Figure 6). The hiding of the key can use any algorithm, and it is obvious to use the NP-hard problem algorithm as it was a well-known algorithm at the time of invention. The hiding of the key makes the transmission of the keys more secure and makes the compromising of the key and the encrypted data difficult. Therefore it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to hide the key data within the attachment file to make the location of the key information extremely difficult.

Claim 17 is rejected as applied above in rejecting claim 12. Furthermore, Leppek discloses:

The method of claim 12 further including the step of discarding the dual-encrypted blocks after decryption with the secondary keys (column 6, lines 10-14), wherein the data stream is not stored (discarded) at the recipient side.

Claim 18 is rejected as applied above in rejecting claim 11. Leppek does not explicitly disclose the step of transmitting an e-mail message to a provider of the encrypted data file, the message having a status content. Watts teaches a system where an electronic message (e-mail) is transmitted to a customer along with an attachment "key-file" which has the keys necessary to access the encrypted data (Figure 2, column 4 lines 37 – 47). In the method of Leppek, the multiple encrypted data is sent over a network to a receiver which must possess multiple keys (decryption operations) to decrypt the multiple encrypted data. Leppek does not explicitly disclose the method of distributing the unique keys to the receiver, but Leppek reveals that two different keys would be required to decrypt a twice encrypted data (column 6, lines 40-49). It was well-known at the time of invention that e-mails with attachment files are a common way to send data files to users. Leppek also discloses that the receiver needs the decryption operators in a correct order in order for the decryption to work properly (Leppek: column 6, lines 41-49). Therefore it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to each type of data with its corresponding key in an attachment file so that the data file could be decrypted if it is encrypted with more than one key that the receiver does not possess (Watts: column 52-55).

6. Claims 6-7, and 21-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leppek (U.S. Patent 5,933,501) in view of Watts (U.S. Patent 6,587,842) in further in view of Cane et al. (U.S. Patent 6,754,827).

Claim 6 is rejected as applied above in rejecting claim 5. Furthermore, Leppek discloses:

formatting the secondary keys as a data structure (column 5, lines 34-45).

Leppek and Watts do not explicitly teach encrypting the secondary keys with the master key. Cane teaches encrypting secondary keys with a master key (Figure 2) before transmitting the key over a network. Cane states that encrypting the secondary keys with the master key allows access control and provides security and higher assurance of data integrity due to the lower probability of compromising the key (column 2 lines 25 – 55). The system of Leppek-Watts may transmit the keys and the data file over a data network, such as the Internet, which could be susceptible to interception. It is obvious that that security and integrity are necessary and providing an extra level of security by encrypting the keys would have been obvious to one of ordinary skill in the art at the time of invention to stymie attempts to intercept and decipher the data file.

Claim 7 is rejected as applied above in rejecting claim 6. Leppek and Watts do not explicitly teach encrypting the secondary keys with the previous key. Cane teaches encrypting secondary keys with a master key (Figure 2) before transmitting the key over a network. Cane states that encrypting the secondary keys with the master key allows access control and provides security and higher assurance of data integrity due to the lower probability of compromising the key (column 2 lines 25 – 55). The system of Leppek-Watts may transmit the keys and the data file over a data network, such as the

Internet, which could be susceptible to interception. It is obvious that that security and integrity are necessary and providing an extra level of security by encrypting the keys would have been obvious to one of ordinary skill in the art at the time of invention to stymie attempts to intercept and decipher the data file.

Claim 21 is rejected as applied above in rejecting claim 11. Leppek and Watts do not explicitly teach encrypting the secondary keys with the previous key. Cane teaches encrypting secondary keys with a master key (Figure 2) before transmitting the key over a network. Cane states that encrypting the secondary keys with the master key allows access control and provides security and higher assurance of data integrity due to the lower probability of compromising the key (column 2 lines 25 – 55). The system of Leppek-Watts may transmit the keys and the data file over a data network, such as the Internet, which could be susceptible to interception. It is obvious that that security and integrity are necessary and providing an extra level of security by encrypting the keys would have been obvious to one of ordinary skill in the art at the time of invention to stymie attempts to intercept and decipher the data file.

Claim 22 is rejected as applied above in rejecting claim 21. Leppek and Watts do not explicitly teach encrypting the secondary keys with the previous key. Cane teaches encrypting secondary keys with a master key (Figure 2) before transmitting the key over a network. Cane states that encrypting the secondary keys with the master key allows access control and provides security and higher assurance of data integrity due to the

lower probability of compromising the key (column 2 lines 25 – 55). The system of Leppek-Watts may transmit the keys and the data file over a data network, such as the Internet, which could be susceptible to interception. It is obvious that that security and integrity are necessary and providing an extra level of security by encrypting the keys would have been obvious to one of ordinary skill in the art at the time of invention to stymie attempts to intercept and decipher the data file.

Claim 23 is rejected as applied above in rejecting claim 22. Leppek and Watts do not explicitly teach encrypting the secondary keys with the previous key. Cane teaches encrypting secondary keys with a master key (Figure 2) before transmitting the key over a network. Cane states that encrypting the secondary keys with the master key allows access control and provides security and higher assurance of data integrity due to the lower probability of compromising the key (column 2 lines 25 – 55). The system of Leppek-Watts may transmit the keys and the data file over a data network, such as the Internet, which could be susceptible to interception. It is obvious that that security and integrity are necessary and providing an extra level of security by encrypting the keys would have been obvious to one of ordinary skill in the art at the time of invention to stymie attempts to intercept and decipher the data file.

Claim 24 is rejected as applied above in rejecting claim 21. Leppek and Watts do not explicitly teach encrypting the secondary keys with the previous key. Cane teaches encrypting secondary keys with a master key (Figure 2) before transmitting the key over

a network. Cane states that encrypting the secondary keys with the master key allows access control and provides security and higher assurance of data integrity due to the lower probability of compromising the key (column 2 lines 25 – 55). The system of Leppek-Watts may transmit the keys and the data file over a data network, such as the Internet, which could be susceptible to interception. It is obvious that that security and integrity are necessary and providing an extra level of security by encrypting the keys would have been obvious to one of ordinary skill in the art at the time of invention to stymie attempts to intercept and decipher the data file.

7. Claims 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leppek (U.S. Patent 5,933,501) in view of Watts (U.S. Patent 6,587,842) in further in view of Wu et al. (U.S. Patent 6,374,363).

Claim 19 is rejected as applied above in rejecting claim 11. Leppek does not explicitly disclose the step of adding footprint files to a host system, the footprint files enabling detection of copying of the encrypted data file. Wu discloses a method of adding footprint files on a host system comprising comparing the footprint files to files to see if the files are the same or different (column 3 line 43 – column 4 line 8). This provides the benefit of discovering if the file already exists, and can detect if a copy was made on the same host system. The detection of copying of the file is another security measure to discover illegal copying of files, such as the files of Leppek, so that it can be detected and stopped. Therefore it would have been obvious to one of ordinary skill in the art at

the time the invention was made to use footprint files to detect the illegal copying of the files of Leppek, and thereby providing another measure to protect the integrity of the data being transmitted.

Claim 20 is rejected as applied above in rejecting claim 11. Leppek does not explicitly disclose the step of adding footprint data to files to a host system. Wu discloses a method of adding footprint files on a host system comprising comparing the footprint files to files to see if the files are the same or different (column 3 line 43 – column 4 line 8). This provides the benefit of discovering if the file already exists, and can detect if a copy was made on the same host system. The detection of copying of the file is another security measure to discover illegal copying of files, such as the files of Leppek, so that it can be detected and stopped. Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to use footprint files to detect the illegal copying of the files of Leppek, and thereby providing another measure to protect the integrity of the data being transmitted.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KA 6/29/07

KA
06/29/2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100